SAVIS®

TRUSTED ARCHIVE 1.0

Increasingly, business processes are being carried out electronically, and thus the volume of electronic documents to be processed is growing. For most companies there arises not only the necessity of efficiently processing these documents, but also the question of how to archive them and ensure their legal validity. E-documents must guarantee that they have the same probative value as their paper counterparts.

Trusted Archive 1.0 offers a solution for electronic documents long term archiving that ensures readability and trustworthiness based on the application of modern standards using electronic signatures/seals and timestamp security features. The archiving process is based on general principles for working with documents and legislative requirements. Documents are automatically maintaining long-term validity.

The solution offers easy and fast setup of archival and destruction rules covering needs, that arise when an organization uses electronic documents. The system provides support for the standardization of work with documents for long-term use as legally relevant evidence and thus enhances legal certainty in all key business processes.

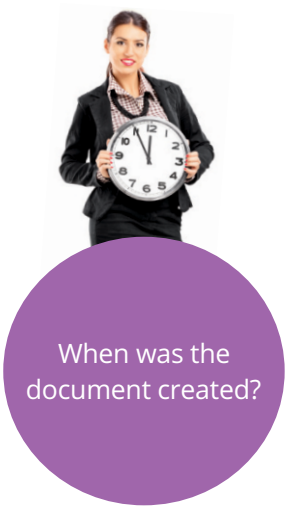
Trusted Archive 1.0 represents a specific type of application, that offers support for the entire archival process and includes the following features:

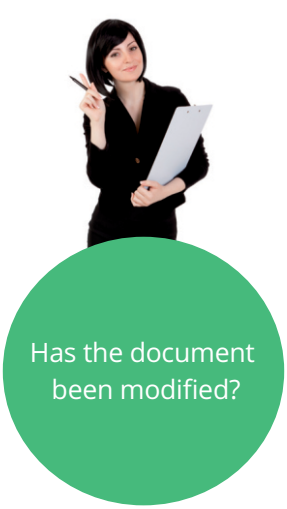
- ✔ Documents manual loading
  Automated loading of documents from a source information systems using web services
- ✔ Security elements (electronic signatures and time-stamps) based on qualified certificates validation
- ✔ Archiving documents in long term archival packages, including timestamping
- ✔ Cost savings due to possibility of grouping random documents into archival packages
- ✔ Ensures periodic validity extension by means of automatic re-stamping
- ✔ Configurable archival and destruction rules for different document types
- ✔ Obtaining and storing all relevant validity evidence of the stored documents
- ✔ Automated documents destruction according to configurable rules
- ✔ Searching and displaying of documents

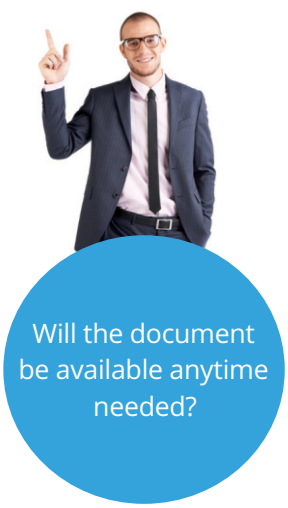
Benefits

- ✔ Ensuring long-term legal relevance of archived documents
- ✔ Unified storage of all document types
- ✔ Streamlining the process of archived documents management
- ✔ Reducing the risk of loss or unauthorized destruction of documents
- ✔ Wide range of integration possibilities with existing infrastructure in a company

TRUSTED ARCHIVE 1.0







Long-Term Archiving Principles

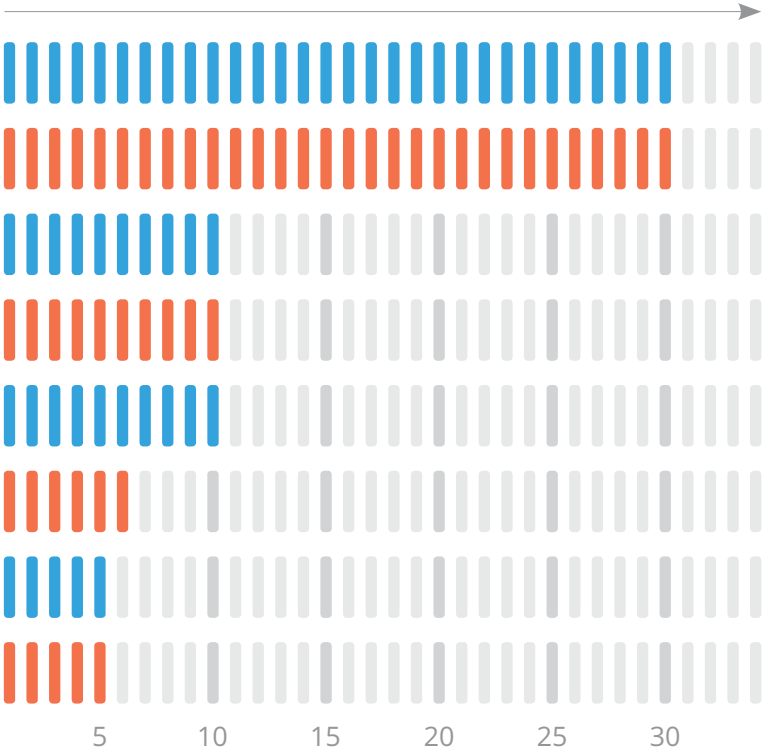
The archiving process in Trusted Archive 1.0 is based on document storage general principles and legislative requirements to ensure long-term electronic documents credibility.

Authenticity
Proof of who was the document real author and preservation of its indisputability.

Credibility
Provision of a trustworthy environment for working with electronic documents, which is based on processes ensuring objective proofs and non-repudiation for stored documents.

Legibility
Ensurance of integrity, availability an content unchangeability of a document and its metadata during his life cycle. Which is achieved by using appropriate inteligent hardware system designed for long-term unstructured data storage.

Indisputability
Storing verifiably unchanged document, that can be safely used any time regardless of its nature and means of storage.



Solution Benefits

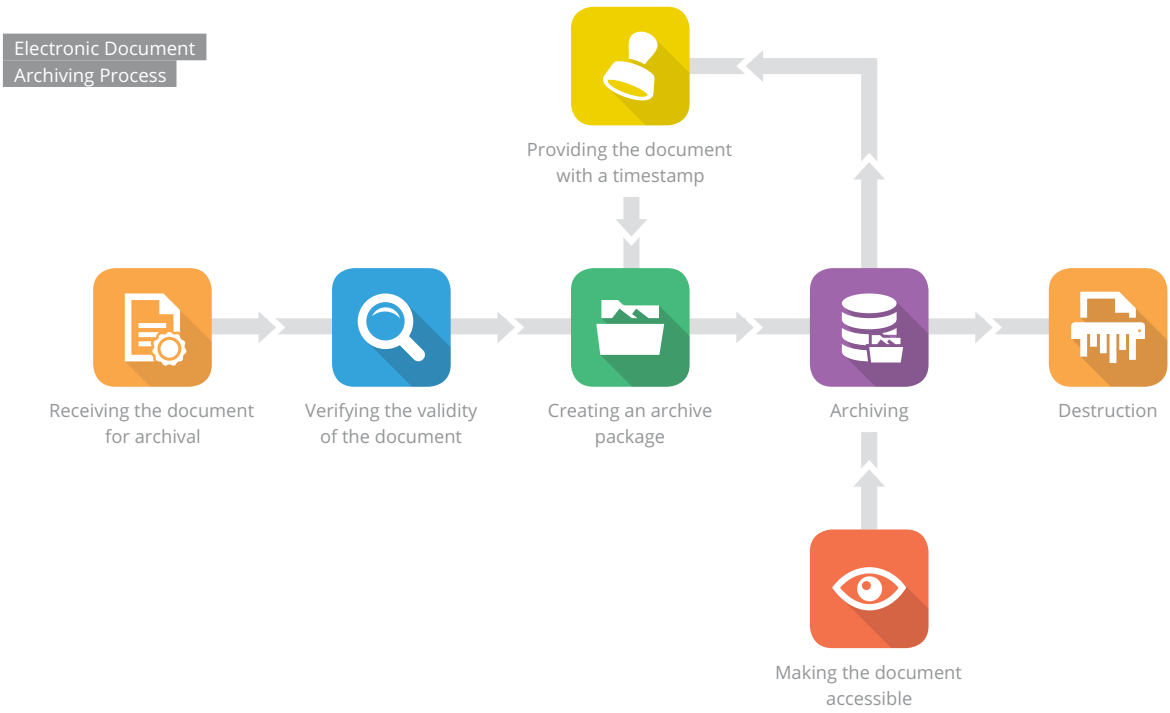
Verifying the Authenticity and Integrity of Documents
Security elements and validation data are mainly electronic signatures based on qualified certificates ensuring document's integrity and autenticity, and qualified timestamps proving document's undeniable existence in time. For this validation Trusted Archive 1.0 utilizes the public service CertReview, that guarantees verification of qualified certificates throughout the EU.

Ensurance of Document Long-Term Legal Validity
Trusted Archive 1.0 provides assurance that the documents will be stored in accordance with applicable legislation and will have sustainable legal relevance. Long-term sustainability of the stored documents legal relevance is based on:

- ✔ Electronic signatures / seals as tools to ensure data integrity and incontrovertibility
- ✔ Hashes as permanent and unique document identifiers
- ✔ Long-term custody for document's electronic signatures and timestamps
- ✔ Ensuring the integrity of documents and information about their archivation
- ✔ Preservation of validation data for documents stored in archival packages (AIP) verification
- ✔ Provision of evidence of document autenticity for the needs of the author and jurisdiction

The key to the fulfilment of the above principles is the creation of so-called archival

TRUSTED ARCHIVE 1.0



packages that are generated in formats based on the European ETSI standards. Through their use, separate documents as well as groups of documents can be saved utilizing archival rules. For example, all invoices received in asingle day or the individual records of the documents.

Efficiency Increase

Trusted Archive 1.0 integration to the company infrastructure ensures trustworthy archivation of electronic documents and hence their legal relevance comparable to the paper-based douments. This way it is possible to work only with electronic documents and eliminate complicated paper-based document management processes.

Central Administration

Trusted Archive 1.0 is an autonomous solution that communicates with other systems via web services. Thus it can easily be integrated into aheterogeneous IT infrastructure at any organization, which reduces the cost of implementing links to other systems and protects investments into existing technologies.

Ensuring Security

Trusted Archive 1.0 Solution is based on modern cryptographic methods using standard security features. Documents are stored securely; additional information (metadata) is stored in asimilar way to the documents. All operations with the documents are logged and audited. Great emphasis is placed on access control, which rules out any tampering with the data.

The system allows installation with a minimum model of 02 nodes, ensuring high availability, load balancing.

Ensure the integrity and reliability when archiving documents, do not allow changing or deleting original documents after they has been archived.

Data self-protection mechanism including automatic data error detection and allowing data recovery when an error occurs.

Digital data storage allows organization into separate virtual zones with decentralized administration as well as independent access for different units.

Enables encryption of important and sensitive data with the most advanced algorithms such as AES, 3DES...

Supports different types of storage connection standards as NFS, CIFS, WebDAV protocols, S3 Protocol....

Encapsulate data packets for permanent storage according to OAIS AIP standard, and compatible with eIDAS long-term electronic archiving standard.

Checking and validating digitally signed documents, digitally signed for permanent storage/permanent digital signature (LTV) for digital archives.

Store and record authentication data and allow checking, retrieval... to ensure proof-of-evidence

Advanced search function, full-text search function allows to display full details of stored information such as metadata, document information validate stamp/store authentication....for each type electronic document.

Advanced search function, full-text search function allows to display full details of stored information such as metadata, document information validate stamp/store authentication....for each type electronic document.

Allows to download metadata, log, and event information.

Configure notifications to allow sending emails, notifications...

Packaged documents will be automatically processed and put into archives in an archive format that ensures long-term archive, long-term authentication, and an archive format that ensures long-term archival standards before digital signning or packaging (PDF/A)

The system allows updating, archiving, uploading documents from other systems via Web Service API such as e-Doc, Web, SIP, Ingest...

Ensure security for digital signing components such as digital signatures, timestamps, long-term advanced authentication digital signatures... for long-term archive and verification of archived documents.

Archive electronic documents according to LTA long-term storage packaging standards including Timestamps (LTANs)

TRUSTED ARCHIVE 1.0

Centralised Management of Archived Documents

Has function to ensure auto-renewal of timestamp

Allows configuring different archiving and destruction scheduling rules.

Allows storing authentication information and checking validation, relevant evidence to put into archiving.

Automatically destroy documents according to established policies/rules configuration.

Allows to set a policy to retain archives when the expiration date has expired or the decision is made to switch to permanent archives.

Allow decentralization, approval to download archived documents.

Export and download the archival historical evidence information of a document

Provide CertReview service that allows to check digital certificates of CAs such as CRL, verify digital certificate term for long-term archive of digital signatures...

Allowing to store and verify many long-term storage formats according to standards: PAdES, XAdES, CAdES...

Integrated time-stamped signing for long-term authentication of electronic records according to LTV standards and LTANS standard digital signature for long-term storage and authentication of electronic documents.

Integration with e-Seal system, HSM digital signing, local digital signing using USB Token ... of many different CAs, many different TSAs for different purposes of stamping authentication and storing electronic documents.

Integration with other systems

Trusted Archive 1.0 offers various tools for integration, both for input of documents and for controlling subsequent processes such as destruction or providing documents from the archive.

Basic integration tools:

- ✔ Trusted Archive 1.0 's own API (web services)
- ✔ Services for input of documents via a shared file system
- ✔ Support for native communication with selected information systems (typically web services)

With regard to native integration interfaces, there are various specialised adapters for different types of system:

- ✔ Document management systems
- ✔ Enterprise information and accounting systems
- ✔ Record management systems

Allows the collection of documents from many different filing sources: the digitized scanner has been packed with the corresponding metadata, copied to the filing folders allowing automatic collection of archived documents

Allows selection, collection of documents submitted from the Files System folders or shared files on the network environment

Allows integration with advanced SIP OAIS packaging submission modules via API Web Service or any other electronic document management system, electronic archiving into a long-term digital archive (Long-term preservation).

Able to archive different types of Dell, EMC, Netapp storage from NAS, Object Storage

TRUSTED ARCHIVE 1.0

Able to integrate with insurance model, secure storage via LTO private tape library (LTFS)

Able to integrate with Cloud Storage systems via API, S3 protocol such as MinIO, AWS...

Legislation and Standards

Trusted Archive 1.0 respects the legislative requirements of the laws of EU regarding working with el. documents and their long-term storage.

- ✔ Regulation (EU) No 910/2014 - EIDAS
- ✔ Comminssion decision 2011/130/EU

The solution is based on proven standards for the administration and archiving of documents.

- ✔ OAIS (Open Archival Information System, ISO 14721)
- ✔ ETSI TS 101 903 XML Advanced Electronic Signatures (XAdES)
- ✔ ETSI TS 101 733 CMS Advanced Electronic Signatures (CAdES)
- ✔ ETSI TS 102 923 PDF Advanced Electronic Signatures (PAdES)

Formats for Long-term Documents Archiving

XAdES

The format XAdES is based on XML and the format XMLDSig extended to XAdES, which is used as a standard for official communica tion within the European Union. XAdES is standardized by ETSI TS 101 903.

CAdES

The secure format CAdES (CMS Advanced Electronic Signatures) is standardized by ETSI TS 101 733. It provides electronic signatures in the form of binary data. Like XAdES, it supports various document formats.

PAdES

PAdES is the name of a PDF document format that allows the insertion of modified electronic signatures that are expanded to include a section for writing metadata, and storage of the individual certificates, certifi - cate revocation lists and verification results. PAdES is standardized by ETSI TR 102 923.

Technologies Used

The solution guarantee reliability and make it a comprehensive system for archiving documents. The basic Trusted Archive 1.0 implementation is intended to runwith the following components:

- ✔ A database and application server
- ✔ A disc array/repository – the size and type depend on the expected volume of data
- ✔ A backup device/library – the size and type depend on the expected volume of data and the standards of the organization

Additionally the solution can be used to centrally manage keys and digital certificates, including support for the physical storage of security features using HSM (Hardware Security Modules).

Production Environment

Trusted Archive 1.0 is supplied as a comprehensive solution, preinstalled on a standardized server or in apublic data centre in the form of aprivate cloud service. Operation is also possible within a customer's infrastructure that meets the recommended configuration.

SAVIS®

CÔNG TY CỔ PHẦN CÔNG NGHỆ SAVIS

Trụ sở chính: Tầng 9, tòa nhà Việt Á, số 9 phố Duy Tân, Phường Dịch Vọng Hậu, Quận Cầu Giấy, TP. Hà Nội
Văn phòng đại diện: Tầng 2, tòa nhà WinHome, số 25 đường Đào Duy Anh, Phường 9, Quận Phú Nhuận, TP. Hồ Chí Minh, Việt Nam
Website: www.savis.vn I Email: dichvuso@savis.vn I Phone: +(84-24) 3782 2345 I Hotline: 1900 636156